453-SRD-SWSI

450/MISSION SERVICES PROGRAM OFFICE

Space Network (SN) Web Services Interface (SWSI) System Requirements

Original

Effective Date - February 2001

Expiration Date - February 2006

National Aeronautics and
Space Administration

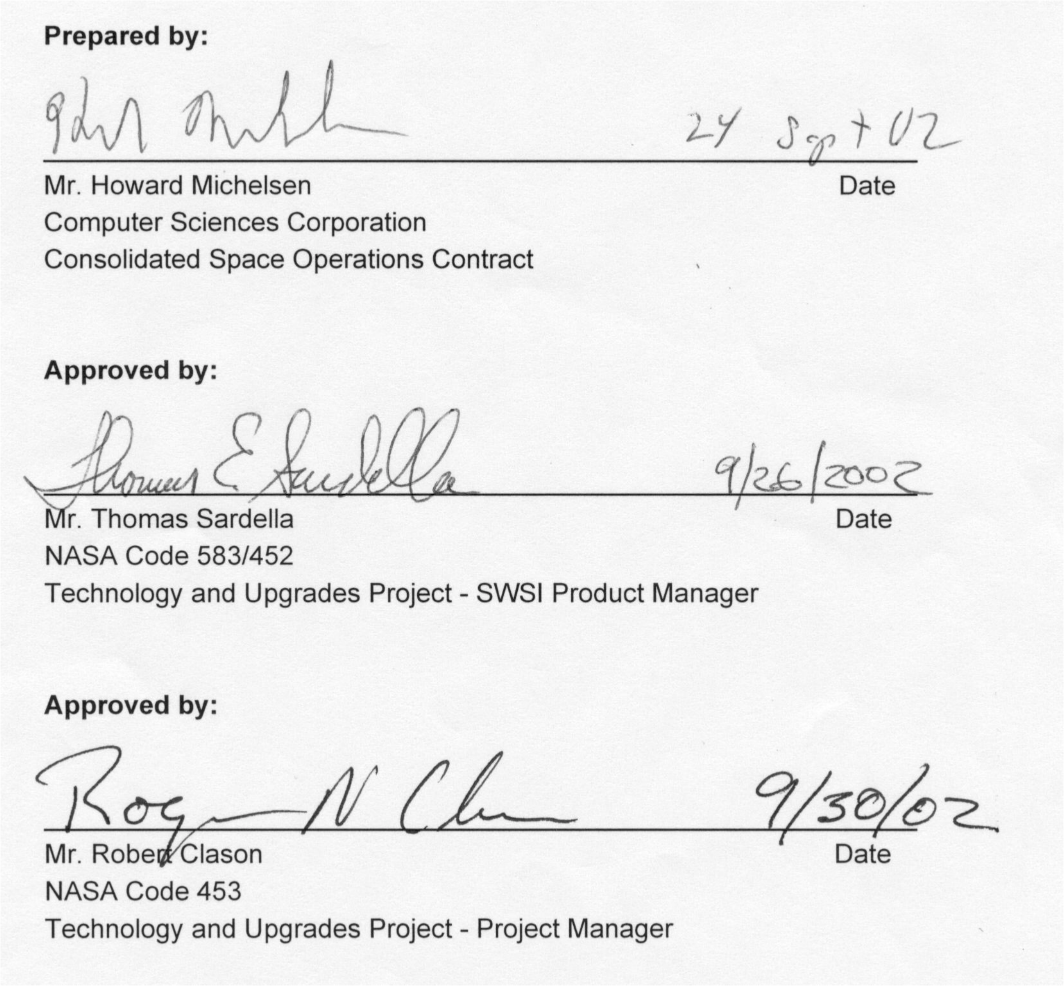
Goddard Space Flight Center
Greenbelt, Maryland

CHECK THE GSFC CENTRALIZED CONFIGURATION MANAGEMENT SYSTEM AT:
http://gdms.gsfc.nasa.gov
PRIOR TO USE TO VERIFY THAT THIS IS THE CORRECT VERSION

Space Network (SN)
Web Services Interface (SWSI)
System Requirements

Original

February 2001



Prepared by:

24 Sept 02

Mr. Howard Michelsen Date
Computer Sciences Corporation
Consolidated Space Operations Contract

Approved by:

9/26/2002

Mr. Thomas Sardella Date
NASA Code 583/452
Technology and Upgrades Project - SWSI Product Manager

Approved by:

9/30/02

Mr. Robert Clason Date
NASA Code 453
Technology and Upgrades Project - Project Manager

Goddard Space Flight Center
Greenbelt, Maryland

Preface

This *Space Network (SN) Web Services Interface (SWSI) System Requirements* document specifies the requirements for the SWSI product.

This document is under the configuration management of the Flight Programs and Projects Directorate's Technology and Mission Upgrades Project (Code 453) Configuration Control Board (CCB). Configuration Change Requests (CCR) to this document may be submitted to the Technology and Mission Upgrades Project's CCB along with supportive material justifying the proposed change. Changes to this document will be made by Document Change Notice or by complete revision.

Questions and proposed changes concerning this SWSI System Requirements document may be addressed to:

SWSI Product Manager

Technology and Mission Upgrades Project
Code 453
Goddard Space Flight Center
Greenbelt, MD 20771

Change Information Page

List of Effective Pages	
Page Number	**Issue**
Title	Original
ii through ix	Original
1-1 through 1-3	Original
2-1 through 2-4	Original
3-1 through 3-10	Original
4-1 through 4-14	Original
5-1 through 5-4	Original
6-1	Original
7-1 through 7-2	Original
AB-1 through AB-3	Original

Document History			
Document Number	**Status/Issue**	**Publication Date**	**CCR Number**
453-SRD-SWSI	Original	February 2001	453/035

DCN Control Sheet

DCN Number	Date/Time Group (Teletype Only)	Month/Year	Section(s) Affected	Initials

Contents

Section 1. Introduction

Section 2. SWSI Architecture

Section 3. System Requirements

Section 4. Functional Requirements

Section 5. Operations and Maintenance (O&M)

Section 6. Documentation

Section 7. Training

Figure

Abbreviations/Acronyms

Section 1. Introduction

1.1 Purpose

This *Space Network (SN) Web Services Interface (SWSI) System Requirements* document specifies the requirements for the SWSI product.

The SWSI provides SN customers with a standards-based and readily available Web interface that allows them to acquire SN services by interacting with the Network Control Center Data System (NCCDS) or the Demand Access System (DAS).

The NCCDS allows SN users to acquire all types of SN services both individually and in valid combinations such as a coherent pair of forward and return services, or a return service and a tracking service based on the return service. As currently planned, the DAS is limited to providing only Multiple Access Return (MAR) services. However, the DAS uses newer technology that greatly expands the number of available MAR services. This expansion in the number of MAR services and various other operational features makes use of the DAS an attractive option for SN customers who require continuous support or who need to request support very shortly before the needed support period and with a minimum of scheduling effort.

For SN services provided via interaction with the NCCDS, the SWSI provides a simple low-cost interface option for SN customers who do not require the full set of features provided by more complex systems such as the User Planning System (UPS). This would include suborbital and other infrequent SN customers; however, use of the SWSI by other users is not precluded.

The SWSI provides the only available customer interface to the DAS.

1.2 Background

The interface between a customer Mission Operations Center (MOC) and the NCCDS consist of electronically exchanged formatted messages. New SN customers have traditionally been provided with a limited number of options for implementing this interface. A full-featured SN scheduling tool is provided by the UPS, which runs on a Hewlett-Packard (HP) Unix host. New customers desiring to use UPS for scheduling must either purchase their own system at a significant cost or interface with an institutional UPS located within Goddard Space Flight Center (GSFC) Multisatellite Operations Control Center (MSOCC). A NASA Integrated Services Network (NISN) Closed Internet Protocol (IP) Operational Network (IONet) connection is required for the latter option. No standard option exists to provide a real-time reconfiguration and performance data monitoring interface. All SN customers have been required to implement their own real-time systems at considerable cost.

Prospective SN customers have brought to light the need for a simple, standard, readily available interface to the NCCDS. In response to this need, the National Aeronautics and Space Administration (NASA) funded an in-house effort to determine the feasibility of such a tool. This effort resulted in a prototype of a web-based cross-platform customer interface to the NCCDS, called SWSI. Prototyping and proof of concept work was completed and has been used to provide support to the Long Duration Balloon Project (LDBP).

The final operational SWSI is a follow-on to the prototype effort and provides improvements in the form of a Graphical User Interface (GUI) and better management of user schedule information. The intent of SWSI is to provide SN customers with an interface to the NCCDS from a desktop computer or workstation without the cost of a custom implementation, and to provide access either from the NISN Closed IONet or via the NISN Open IONet. Since the Open IONet allows access from other networks such as the NASA Science Internet and from the public Internet, this will allow use of the SWSI by NASA's university, enterprise, and inter/intra-agency partners.

In addition, the development of the DAS requires a corresponding customer interface. The SWSI will seamlessly provide this DAS interface integrated with the NCCDS interface.

The SWSI will be installed within the Network Control Center (NCC). Based on current schedules, the SWSI will begin operation shortly after the completion of the transition of the NCC facility from GSFC to the Data Services Management Center (DSMC) at the White Sands Complex in New Mexico in 2002.

1.3 Scope

This document addresses the system, functional and performance, operations and maintenance, documentation, and training requirements for SWSI. As organized herein, system requirements include requirements for external communications, installation, security, test and user interface; and operations and maintenance requirements include requirements for reliability, maintainability, and availability.

1.4 Reference Documents

a. *Maintainability Program for Systems and Equipment*, MIL-HDBK-470.

b. *Maintainability for Verification/Demonstration/Evaluation*, MIL-HDBK-471.

a. *NASA Procedures and Guidelines for Security of Information Technology*, NPG 2810.1, August 1999

b. *GSFC Security Manual*, GHB 1600.1B.

c. *NASA Safety Policy and Requirements Handbook*, NHB 1700.1.

d. *Interface Control Document Between the Network Control Center Data System and Mission Operations Center*, 451-ICD-NCCDS/MOC.

e. *Interface Control Document between the Demand Access System and the Space Network Web Services Interface*, 451-ICD-DAS/SWSI

f. *Data Services Management Center (DSMC) System Requirements Specification for the Network Control Center Data System (NCCDS)*, CSOC-CEN.SE11.001070.

g. *Network Systems Integration & Analysis Master Test Plan for Network Control Center Data Systems*, CSOC-GSFC-TEST-000924.

h. *IP Operation Network (IONet) Security Plan*, 290-003.

i. *NISN Project Security Plan*, N/A.

j. *Space Network (SN) User's Guide*, 450-SNUG.

k. *Transition Readiness Process*, CSOC-CEN.PO50.001028

l. *The Java*^{TM} *Virtual Machine Specificatio*n -- available at: http://java.sun.com/docs/books/vmspec/2nd-edition/html/VMSpecTOC.doc.html

m. *Data Services Management Center (DSMC) Transition Plan*, CSOC-CEN.PLAN-000855

n. Internet Protocol Operational Network (IONet) Access Protection Policy and Requirements, 290-004

Section 2. SWSI Reference Architecture

2.1 Introduction

Figure 2-1 depicts the SWSI reference architecture. Herein, this reference architecture serves only to facilitate discussion of the SWSI. The reference architecture, itself, is not a requirement. However the basic assumptions underlying the SWSI reference architecture do, in effect, preclude implementation of the SWSI with a significantly different architecture.

2.2 Underlying Assumptions

The following assumptions are the basis for the SWSI reference architecture:

a. Client-server partitioning of the SWSI is a cost-effective approach for providing the SWSI capabilities to SN customers. It is assumed that some SWSI applications client software will run on the customer's desktop computer or workstation rather than just a generic Web browser. However, this document does not explicitly partition SWSI functional requirements between the SWSI server and the SWSI client.

b. The SWSI must include both servers on both the Open IONet and the Closed IONet. SWSI clients on the Open IONet and the Internet are provided service indirectly to the SWSI servers on Closed IONet via the SWSI servers on Open IONet. This is necessary because:

   1. The Secure Gateway separates the Closed IONet from the Open IONet.

   2. The NCCDS and DAS are located on the Closed IONet.

   3. Some SWSI clients are located on the Open IONet.

c. The SWSI's Reliability, Maintainability, Availability (RMA) requirements cannot be satisfied without providing prime and backup servers.

2.3 SWSI Components

The SWSI reference architecture partitions the SWSI into the following components:

a. SWSI Client Workstation. The SWSI client workstation is the platform provided by the user, and includes the hardware and software infrastructure necessary to host the SWSI client software. This client software is part of the SWSI product and provides users with the capability to acquire SN services via connections with either the SWSI Open Server or the SWSI Backend Server.

b. SWSI Servers. The SWSI servers act as proxies to route requests from the SWSI client to the NCCDS and/or the DAS and return responses to the client. The details of this process vary depending on whether the SWSI client is located on the open or closed side of the IONet Secure Gateway.

1. SWSI Open Server. This server is on the open side of the IONet Secure Gateway. It connects to SWSI clients on the open side of the IONet Secure Gateway and to the SWSI Backend Server on the closed side of the IONet Secure Gateway.

2. SWSI Backend Server. This server is on the closed side of the IONet Secure Gateway. It connects to SWSI clients, the NCCDS and the DAS on the closed side of the IONet Secure Gateway, and to the SWSI Open Server on the open side of the IONet Secure Gateway. The formats and protocols applicable to connections between the SWSI Backend Server and the NCCDS are specified in 451-ICD-NCCDS/MOC. The formats and protocols applicable to connections between the SWSI Backend Server and the DAS are specified in 451-ICD-DAS/SWSI.

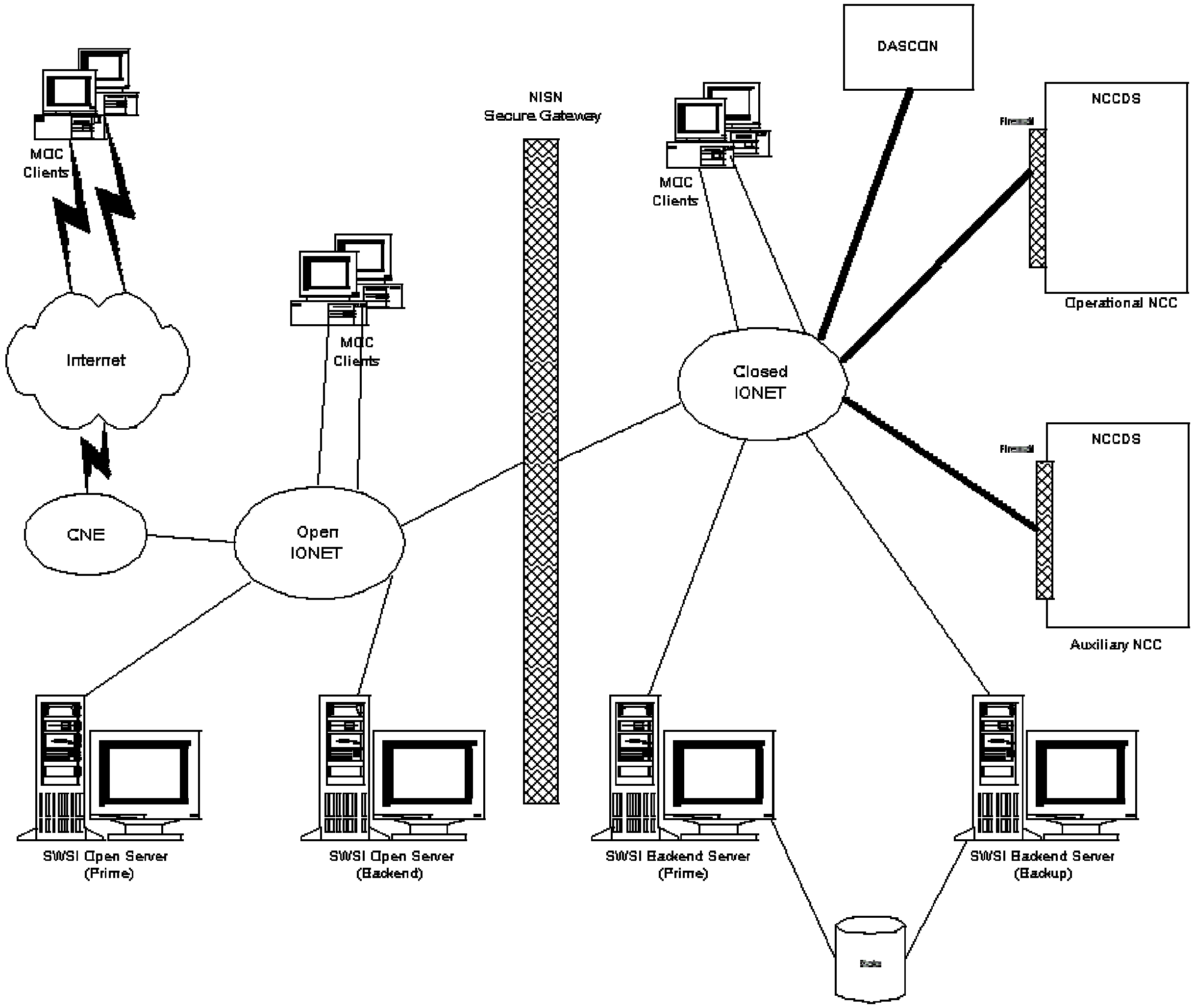


Figure 2-1. High Level SWSI Architecture

2.4 External Elements

The SWSI reference architecture places the SWSI in an environment comprising the following external elements:

a. Internet. The user can access SWSI via the NASA Science Internet or the public Internet.

b. CNE. The Center Network Environment (CNE) is the non-mission critical computer network at GSFC.

c. IONet. In contrast to the CNE, the IONet is used for mission operations. The IONet is divided into two parts separated by the IONet Secure Gateway. Customer systems connected to the Closed IONet are not permitted to be connected to any other network, whereas customer systems connected to the Open IONet may also be connected to other networks.

d. IONet Secure Gateway. The IONet Secure Gateway is a rule-based firewall used to prevent penetration of hosts on the Closed IONet from less secure networks.

e. NCCDS. The NCCDS in the operational NCC environment allows SN customers to schedule, reconfigure, and monitor SN services. A separate NCCDS in the Auxiliary NCC (ANCC) environment supports interface testing and can be used as a backup when the operational NCCDS is unavailable. The SWSI is capable of maintaining simultaneous connections with both of these NCCDSs

f. DAS. The DAS allows SN customers to schedule, reconfigure, and monitor a limited subset of SN services. The SN's resources are partitioned such that the DAS's activities do not conflict with the NCCDS's activities.

Section 3. System Requirements

3.1 Introduction

This section specifies the following categories of system requirements for the SWSI:

a. Software

b. System Components

c. External Interfaces

d. Installation

e. Security

f. Testing

g. User Interface

3.2 Software

3.2.1

The SWSI includes both off-the-shelf software and custom developed software. Off-the-shelf software applicable to the SWSI includes an operating system, a database management system, network communications software, and software development tools. In all cases, it is intended that the resultant SWSI product maximize portability and hardware independence. With the exception of the following explicit requirements, all SWSI software requirements will be derived by lower level SWSI documents from other requirements (e.g., functional requirements) specified herein.

3.2.2

Any SWSI software to be hosted on the SWSI client shall validly execute on any client platform supporting the Java 2.0 Virtual Machine.

3.2.3

Any SWSI software to be hosted on the SWSI client shall be packaged such that it can be distributed to and/or accessed by users via electronic media.

3.2.4

Custom developed SWSI software shall be designed to facilitate future modifications.

NOTE

> This requirement will be verified by peer review as the software is designed and developed. It is not subject to system test.

3.3 System Components

3.3.1 General

As presented in Section 2, the SWSI reference architecture partitions the SWSI into three components. The following material specifies explicit requirements for these three components. However, it is expected that lower level SWSI documents will derive additional requirements for these components from other requirements (e.g., functional requirements) specified herein.

3.3.2 SWSI Client Workstation

3.3.2.1
The SWSI Client Workstation is the user’s desktop, and will be provided and maintained by the user. The SWSI client is not part of the SWSI product, and is herein excluded from all SWSI requirements (e.g., RMA requirements) that do not specifically include the SWSI client.

3.3.2.2
The SWSI client shall be capable of supporting the Java 2.0 Virtual Machine.

3.3.2.3
For Internet and Open IONet users who will use SN services provided via interaction with the NCCDS, the SWSI Client Workstation shall be capable of establishing and sustaining all connections with the SWSI Open Server applicable to the SWSI's interface with the NCCDS.

3.3.2.4
For Internet and Open IONet users who will use SN services provided via interaction with the DAS, the SWSI Client Workstation shall be capable of establishing and sustaining all connections with the SWSI Open Server applicable to the SWSI's interface with the DAS.

3.3.2.5
For Closed IONet users who will use SN services provided via interaction with the NCCDS, the SWSI Client Workstation shall be capable of establishing and sustaining all connections with the SWSI Backend Server applicable to the SWSI's interface with the NCCDS.

3.3.2.6
For Closed IONet users who will use SN services provided via interaction with the DAS, the SWSI client shall be capable of establishing and sustaining all connections with the SWSI Backend Server applicable to the SWSI's interface with the DAS.

3.3.3 SWSI Open Server

3.3.3.1

For Internet and Open IONet users who will use SN services provided via interaction with the NCCDS, the SWSI open server shall function as a proxy for the SWSI Backend Server. For these users, the SWSI open server shall be capable of establishing and sustaining all connections with the SWSI Backend Server applicable to the SWSI's interface with the NCCDS.

3.3.3.2

As needed, the SWSI open server shall route requests from the SWSI client to the NCCDS and return responses from the NCCDS to the SWSI Client Workstation. In all cases, these exchanges will be via the IONet Secure Gateway and the SWSI backend server.

3.3.2.3

For Internet and Open IONet users who will use SN services provided via interaction with the DAS, the SWSI open server shall function as a proxy for the SWSI Backend Server. For these users, the SWSI open server shall be capable of establishing and sustaining all connections with the SWSI Backend Server applicable to the SWSI's interface with the DAS.

3.3.3.4

As needed, the SWSI open server shall route requests from the SWSI client to the DAS and return responses from the DAS to the SWSI client. In all cases, these exchanges will be via the IONet Secure Gateway and the SWSI backend server.

3.3.4 SWSI Backend Server

3.3.4.1

For Closed IONet users who will use SN services provided via interaction with the NCCDS, the SWSI backend server shall be capable of establishing and sustaining all applicable connections with the NCCDS.

3.3.4.2

For Closed IONet users who will use SN services provided via interaction with the DAS, the SWSI backend server shall be capable of establishing and sustaining all applicable connections with the DAS.

3.3.4.3

For Internet and Open IONet users who will use SN services provided via interaction with the NCCDS, the SWSI backend server shall be capable of establishing and sustaining all applicable connections with the NCCDS. In all cases, these exchanges between Internet and Open IONet users and the SWSI backend server will be via the IONet Secure Gateway and the SWSI open server.

3.3.4.4
For Internet and Open IONet users who will use SN services provided via interaction with the DAS, the SWSI backend server shall be capable of establishing and sustaining all applicable connections with the DAS. In all cases, these exchanges between Internet and Open IONet users and the SWSI backend server will be via the IONet Secure Gateway and the SWSI open server.

3.3.4.5
In support of Internet and Open IONet users, the SWSI backend server shall be capable of establishing connections with the SWSI open server via the IONet Secure Gateway.

3.4 External Interfaces

3.4.1 SWSI Client Workstation

For any combination of Internet, Open IONet and Closed IONet SWSI client users, the SWSI servers shall be capable of supporting simultaneous connections with multiple SWSI clients. Refer to 4.8.1.

NOTE

> Refer to 3.3.2.1. The SWSI Client Workstation is not part of the SWSI product. Therefore this is regarded as an external interface requirement.

3.4.2 IONet Secure Gateway

3.4.2.1
All communications between the SWSI open server and the SWSI backend server shall be channeled through the IONet Secure Gateway.

3.4.2.2
When communicating with each other, the SWSI open server and the SWSI backend server shall not employ protocols or communications techniques that will be blocked by the IONet Secure Gateway.

3.4.2.3

The SWSI shall not require the IONet Secure Gateway to modify its rule set in response to SWSI configuration changes, or in response to the addition or removal of SWSI customers.

3.4.3 Network Control Center Data System

3.4.3.1
For any SWSI client at any time, the SWSI shall be capable of communicating with either the NCCDS located in the operational NCC environment or with the NCCDS located in the ANCC. Refer to 3.7. This implies that the SWSI will be capable of

simultaneously communicating with the operational NCCDS for some clients and with the ANCC’s NCCDS for other clients.

3.4.3.2
All communications between the SWSI and the NCCDS shall comply with 451-ICD-NCCDS/MOC.

NOTE

> 451-ICD-NCCDS/MOC is primarily written as the specification for the interface between a single SN customer and the NCCDS. However, the SWSI is a multi-mission system and 451-ICD-NCCDS/MOC must be interpreted accordingly. For example, message IDs generated by the SWSI do not necessarily have to be unique for the SWSI-NCCDS interface; however, message IDs generated by the SWSI must be unique for each SIC supported by the SWSI.

3.4.3.3
The SWSI shall employ hypertext transfer protocol (HTTP) to retrieve TDRSS Unscheduled Time (TUT) information from the NCCDS. The SWSI shall employ Transmission Control Protocol/Internet Protocol (TCP/IP) for all other communications with the NCCDS. The SWSI will not use Nascom 4800 Bit Block (BB) protocol or File Transfer Protocol (FTP) for any of its communications with the NCCDS.

3.4.3.4
As needed, the SWSI shall establish communications connections with NCCDS services (refer to Table 4-3 of 451-ICD-NCCDS/MOC) and automatically transmit any messages needed to configure the services. In particular, the SWSI shall automatically transmit:

a. Schedule Result Request messages on the NCCDS Schedule Status service connection.

b. User Performance Data Request messages on the NCCDS User Performance Data service connection.

3.4.3.5
For all applicable message formats and message format parameters, the SWSI shall exercise the "full support" customer options. The SWSI will not exercise the "baseline" customer options.

3.4.3.6
For all applicable message formats and message format parameters, the SWSI shall exercise the "normal user" options. The SWSI will not exercise the "Shuttle" options.

3.4.4 Demand Access System

All communications between the SWSI and the DAS shall comply with 451-ICD-DAS/SWSI.

3.5 Installation Requirements

3.5.1 General

The following requirements apply regardless of whether the NCC facility is located at GSFC or within the DSMC at the WSC in New Mexico.

3.5.2 Power Requirements

The SWSI servers shall be capable of successful operation using the power available within the NCC facility. The SWSI servers shall not require either a quantify or quality of electric power that exceeds the capabilities of the NCC facility.

3.5.3 Environmental Requirements

The SWSI servers shall be capable of successful operation within the ambient temperature and humidity ranges available within the NCC facility. The SWSI servers shall not require modification of either the temperature or humidity control capabilities of the NCC facility.

3.5.4 Site Preparation Requirements

3.5.4.1

The equipment installation shall be documented by an Engineering Change (EC).

3.5.4.2

The EC shall list of all necessary power and signal cables.

3.5.4.3

Cable installation shall be in accordance with the requirements of STDN-SPEC-6, GSFC Specification Installation Requirements for STDN Equipment.

3.5.4.4

All cable fabrication shall be in accordance with the requirements of STDN-SPEC-4, Section 3.

3.5.5 Equipment Installation

Equipment installations shall be in accordance with STDN-SPEC-6, Installation Requirements for STDN Equipment.

3.5.5.1

Floor panels shall be in accordance with the requirements of STDN-SPEC-6.

3.6 Security

3.6.1

Both due to the missions it directly supports and to its interface with the NCCDS, the NASA Mission (MSN) information category requirements as defined by the *NASA Procedures and Guidelines for Security of Information Technology*, NPG 2810.1 are applicable to the SWSI.

3.6.2

In the absence of waivers, the SWSI shall satisfy the Baseline Information Technology (IT) Security Requirements applicable to the MSN information category as specified in Appendix A of NPG 2810.1.

3.6.3

For some requirements, waivers may be requested in accord with the provisions of NPG 2810.1.

3.6.4

For all aspects of communications via the IONet, the SWSI shall comply with IP Operational Network (IONet) Security Plan, 290-003 and IP Operational Network (IONet) Access Protection Policy and Requirements, 290-004. However, in case of conflicts between NPG 2810.1, 290-003, and 290-004, 290-003 and 290-004 has precedence.

3.7 Test Requirements

3.7.1

In order to support Engineering Interface (EIF) testing, the SWSI shall provide the capability for SWSI clients to communicate with the ANCC's NCCDS via the SWSI servers.

3.7.2

The SWSI shall provide customers with the capability to segregate their test data from their operational data.

3.8 User Interface

3.8.1 General Features

The SWSI shall provide users of the SWSI Client software with a Graphical User Interface (GUI). The general features provided by the SWSI GUI shall include, but not necessarily be limited to, the following:

a. A main menu or main control panel that can be used to directly, or indirectly, access all available SWSI features.

b. Mechanisms for entry of data into the SWSI.

c. Mechanisms for retrieval of selected information from the SWSI.

d. Presentation of information in a variety of ways including tabular, dynamic, and static.

e. Function selection capabilities including scrolling within windows, hardcopy request, alert acknowledge, enter, and place cursor at any selected screen position.

f. Resizing of a display window without change to the information content of the window.

g. Update of the information content of a window without affect on the information content of other windows.

h. Color-coding of information with redundant (e.g., pattern-coding or shades-of-gray-coding) coding.

i. Presentation of the current time.

j. Tagging of information with the time when it was entered, retrieved, or updated.

3.8.2 SN Services

The SWSI shall provide users of the SWSI client with:

a. All user interface features necessary to support the SWSI functional requirements applicable to NCCDS interactions.

b. All user interface features necessary to support the SWSI functional requirements applicable to DAS interactions.

c. User interface features providing integrated control and information presentation capabilities for operationally related groups of SN services regardless of whether the individual services are provided via interaction with the NCCDS or with the DAS (e.g., integrated presentation of the service configurations of forward services provided via NCCDS interactions and return services provided via DAS interactions).

3.8.3 System Information

The SWSI shall provide users of the SWSI client with:

a. Access to information pertaining to the current status of each applicable SWSI communications connection.

b. Notification when the status of an applicable SWSI connection changes.

c. Access to any available system status information provided by the SWSI servers.

3.8.4 Operator Log On

3.8.4.1 Customer Authorization and Authentication Data

3.8.4.1.1 Maintenance of Customer Authorization and Authentication Data

The SWSI will provide the following capabilities related to the maintenance of customer authorization and authentication data:

a. The SWSI shall provide authorized SWSI administrative personnel with the capability to enter, modify, and delete customer authorization data.

b. The SWSI shall provide authorized SWSI administrative personnel with the capability to review previously entered customer authorization data.

c. The SWSI shall retain customer authorization data until deleted by authorized SWSI administrative personnel.

3.8.4.1.2 Data

The SWSI will retain the following customer data related to operator log on:

a. For each user, the SWSI shall retain a user ID, a password, and a passphrase.

b. For each user, the SWSI shall retain a list of SICs for which the user is authorized.

c. For each combination of user and SIC, the SWSI shall retain a list of valid Support Identifiers (SUPIDENs).

d. For each user, the SWSI shall retain information indicating whether the user interacts with the NCCDS, with the DAS, or both.

e. For each combination of NCCDS user and SUPIDEN, the SWSI shall retain a User ID and Password to be used in messages transmitted to the NCCDS. These User IDs and passwords will not necessarily be the same as the User IDs and passwords used to logon to the SWSI.

NOTE

> The SWSI directly uses the user’s logon user ID in messages transmitted to the DAS. No additional data is needed for this purpose.

3.8.4.2 Log On Process

3.8.4.2.1

The SWSI shall provide authorized users with the capability to logon to the SWSI.

3.8.4.2.2
The SWSI shall validate a user’s logon based on the user ID, password, and passphrase entered by the user.

3.8.4.2.3
Within 10 seconds of its entry, the SWSI shall respond to each logon attempt with an indication of whether it has been accepted or rejected.

3.8.4.2.4
The SWSI shall employ digital certificates in this validation process, and shall rely upon the NASA Certificate Authority to provide digital certificates to SWSI customers.

3.8.4.2.5
The SWSI shall allow connections to be established between a SWSI client and SWSI servers only after a valid user logon from the SWSI client.

3.8.4.2.6
The SWSI shall allow only NCCDS users to access the SWSI NCCDS functions. This includes establishing connections with the NCCDS for the user.

3.8.4.2.7
The SWSI shall allow only DAS users to access the SWSI DAS functions. This includes establishing connections with the DAS for the user.

3.8.4.2.8
For NCCDS users, the SWSI shall provide the user with the capability to select:

a. Connection with either the operational NCCDS or with the ANCC’s NCCDS.

b. Use of operational or test data.

3.8.4.2.9
The SWSI shall provide users with the capability to log-off.

3.8.4.2.10
The SWSI shall maintain a record of currently logged-on users and log of login attempts at all times.

Section 4. Functional and Performance Requirements

4.1 Introduction

This section presents the SWSI requirements for the following:

a. NCCDS Interactions

b. DAS Interactions

c. Database Management

d. Logging

e. System Performance

4.2 NCCDS Interactions

4.2.1 General

4.2.1.1
The SWSI provides SN customers with the capability to interface with the NCCDS to perform the following functions related to SN services:

a. Scheduling

b. Service Reconfiguration

c. Performance Data Monitoring

d. Vector Storage and Transmission

4.2.1.2
In all cases, the SWSI shall ensure that each NCCDS user is precluded from accessing any other user's messages or data.

4.2.2 Scheduling

4.2.2.1 Customer Data Management

For each SIC supported by the SWSI, the SWSI shall provide authorized SWSI administrative personnel with the capability to create and maintain all customer data necessary to perform the scheduling function. In particular, this will include a set of service specification codes (SSCs) corresponding to the set of SSCs maintained for the customer in the NCCDS database, and the list of valid SUPIDENs for the SIC. The SWSI shall provide the user with the capability to review and reference this data in the process of entering schedule requests.

4.2.2.2 Schedule Requests

4.2.2.2.1 General

The SWSI will provide the user with the capability to enter schedule requests and transmit them to the NCCDS as follows:

a. The SWSI shall provide the user with the capability to enter the following types of schedule requests:

   1. Schedule Add Request (SAR).
   2. Schedule Delete Request (SDR).
   3. Schedule Replace Request (RR).
   4. Alternate SAR (ASAR).
   5. Schedule Wait List Request (WLR).

b. Based on the user's logon information, the SWSI shall provide the user with the capability to select the SUPIDEN to be used in the request from a list of SUPIDENs for which the user is authorized.

c. For each of these types of schedule requests, the SWSI shall provide the user with the capability to create a new request by copying and editing a previous request.

d. For each of these types of schedule requests, the SWSI shall provide the user with the capability to use all options specified for that type of request by 451-ICD-NCCDS/MOC.

e. For each of these types of schedule requests, the SWSI shall format the request in compliance with the applicable tables of 451-ICD-NCCDS/MOC. In particular, the SWSI shall not transmit schedule requests to the NCCDS that will result in Schedule Result Messages (SRMs) with a combination of result and explanation codes indicating invalid formatting.

f. The SWSI shall not transmit schedule requests to the NCCDS that will result in a lack of response from the NCCDS due to failure to pass authorization checks.

g. Upon completion of the user's entry of a request, the SWSI shall format, store, and then transmit the request.

h. The SWSI shall retain all stored requests until the request expires according to administrative personnel-specified criteria.

4.2.2.2.2 Schedule Add Request

No additional requirements apply to the entry and transmission of SARs. The SWSI will allow the user to enter and transmit SARs at any time without regard to the relationship of the SAR and any previous schedule request.

4.2.2.2.3 Schedule Delete Request

The following additional requirements apply to the entry and transmission of SDRs:

a. The SWSI shall ensure that each SDR contains a valid reference to an active event, or to a previously transmitted SAR, ASAR, or RR.

b. In order to facilitate this, the SWSI shall provide the user with displays of the current active events and previously transmitted schedule requests.

4.2.2.2.4 Schedule Replace Request

The following additional requirements apply to the entry and transmission of RRs:

a. The SWSI shall ensure that each RR contains a valid reference to an active event, or to a previously transmitted SAR, ASAR, or RR.

b. In order to facilitate this, the SWSI shall provide the user with displays of the current active events and previously transmitted schedule requests.

4.2.2.2.5 Alternate SAR

The following additional requirements apply to the entry and transmission of ASARs:

a. The SWSI shall ensure that each ASAR contains a valid reference to a previously transmitted SAR, ASAR, or RR.

b. In order to facilitate this, the SWSI shall provide the user with displays of previously transmitted schedule requests.

4.2.2.2.6 Schedule Wait List Request

The following additional requirements apply to the entry and transmission of WLRs:

a. The SWSI shall ensure that each WLR contains a valid reference to a previously transmitted SAR, ASAR, or RR and that the previously transmitted SAR, ASAR, or RR has been declined by the NCCDS, i.e., the NCCDS has transmitted an SRM with result code of 02.

b. In order to facilitate this, the SWSI shall provide the user with displays of previously transmitted schedule requests that indicate whether the request has been declined by the NCCDS.

4.2.2.3 TDRSS Scheduling Windows

The SWSI will provide the user with the following capabilities related to TDRSS Scheduling Windows (TSWs):

a. The SWSI shall provide the user with the capability to import files of TSWs into the SWSI. These TSW files must be in a format compatible with the TSW message format specified by 451-ICD-NCCDS/MOC.

b. The SWSI shall provide the user with the capability to select imported TSW files for transmission to the NCCDS.

c. Based on the SIC within each selected file, the SWSI shall verify that the user is authorized to send this TSW data to the NCCDS.

d. For each validly selected file, the SWSI shall format the selected TSWs into one or more valid TSW messages, and transmit them to the NCCDS.

4.2.2.4 TDRSS Unscheduled Time

The SWSI shall retrieve current TDRSS Unscheduled Time (TUT) information from the NCCDS and store it so that it is accessible to Internet and Open IONet SWSI users.

NOTE

> The NCCDS allows all users of the Closed IONet to directly access TUT information, therefore the SWSI does not need to provide TUT information for Closed IONet SWSI users.

4.2.2.5 Schedule Results

4.2.2.5.1 General

In response to schedule requests, the NCCDS will respond with SRMs and with User Schedule Messages (USMs).

4.2.2.5.2 Schedule Result Messages

Upon receipt of an SRM, the SWSI shall:

a. Notify the user that the SRM has been received.

b. Provide the user with the capability to review the SRM.

c. Use the result and explanation codes from the SRM to update the status information for the request or event referenced by the SRM.

d. Provide the user with the capability to review the requests or events with the updated status information.

e. If the result code is 15, delete the referenced event (if any) and annotate the referenced request to indicate that it has been deleted.

4.2.2.5.3 User Schedule Messages

Upon receipt of an USM, the SWSI shall:

a. Notify the user that the USM has been received.

b. Use the USM to update the SWSI’s schedule.

c. Provide the user with the capability to review the updated schedule, including the new USM.

4.2.3 Service Reconfiguration

4.2.3.1 General

The SWSI will provide the user with the capability to enter Ground Control Message Requests (GCMRs) and transmit them to the NCCDS as follows:

a. The SWSI shall provide the user with the capability to enter the following types of GCMRs:

    1. User Reacquisition Request.

    2. User Reconfiguration Request.

    3. Forward Link Sweep Request.

    4. Forward Link Effective Isotropic Radiated Power (EIRP) Reconfiguration Request.

    5. Expanded User Frequency Uncertainty Request.

    6. Doppler Compensation Inhibit Request.

b. Based on the user’s logon information, the SWSI shall provide the user with the capability to select the SUPIDEN to be used in the request from a list of SUPIDENs for which the user is authorized.

c. For each of these types of GCMRs, the SWSI shall provide the user with the capability to use all options specified for that type of request by 451-ICD-NCCDS/MOC.

d. For each of these types of GCMRs, the SWSI shall format the GCMR in compliance with the applicable tables of 451-ICD-NCCDS/MOC. In particular, the SWSI shall not transmit GCMRs to the NCCDS that will result in a GCM Status Message indicating that the GCMR has been rejected by the NCCDS due to invalid formatting or due to reference to an inapplicable service type.

e. The SWSI shall not transmit GCMRs to the NCCDS that will result in a lack of response from the NCCDS due to failure to pass authorization checks.

f. Upon completion of the user’s entry of a request, the SWSI shall transmit and store the request.

4.2.3.2 Current Service Configuration Displays

The SWSI shall provide the user with the capability to review the configuration of each currently active service and to use this information in the entry of GCMRs as follows:

a. For each service type, the service configuration display will provide detailed information at the individual service parameter level. This level of detail is comparable to that of the USM formats specified in 451-ICD-NCCDS/MOC.

b. As of service start time, the information in the service configuration display will reflect the initial state of the service as specified in the applicable USM.

c. Upon a successful service reconfiguration, the information in the service configuration display will updated to reflect the reconfigured parameter or parameters.

4.2.3.3 GCM Status Message

Upon receipt of a GCM Status Message, the SWSI shall:

a. Notify the user that the GCM Status Message has been received, and show whether the status message indicates that a GCMR was rejected by the NCCDS, rejected by WSC, or accepted by WSC.

b. Allow the user to view the GCM Status Message.

c. Update the information used in the service configuration display if the GCM Status Message indicates that the GCMR was accepted by WSC.

NOTE

> For the Forward Link EIRP Reconfiguration Request, an indication that WSC has accepted the GCMR means that WSC will command the TDRS to reconfigure its EIRP. For all other GCMRs, this indication means that WSC has completed the requested reconfiguration.

4.2.3.4 GCM Disposition Message

Upon receipt of a GCM Disposition Message, the SWSI shall notify the user that the GCM Disposition Message has been received, and show whether the message indicates that a reconfiguration request was acknowledged or not acknowledged by WSC.

NOTE

> A GCM Disposition Message (indicating that WSC has failed to acknowledge a reconfiguration request), will be followed by a GCM Status Message (indicating that the NCCDS has received no response from WSC).

4.2.4 Performance Data Monitoring

4.2.4.1 General

In response to messages received from WSC, the NCCDS will transmit the following performance data messages to the SWSI:

a. User Performance Data (UPD) messages.

b. Return Channel Time Delay (RCTD) messages.

c. Time Transfer Messages (TTMs).

d. Acquisition Failure Notification (AFN) messages.

4.2.4.2 User Performance Data Messages

The SWSI will provide the following UPD message capabilities:

a. For each TDRS, the SWSI shall be capable for receiving one UPD message each five seconds for each SWSI user with an active service on that TDRS.

b. Upon receipt of a UPD message, the SWSI shall verify that it applies to a SUPIDEN for which there is a logged-on SWSI user. If it does, the SWSI shall make the information from the UPD message available for presentation to that user in real time.

c. The SWSI shall provide users with the following capabilities and options for the presentation of UPD message information:

   1. Default display formats.
   2. Dynamic updates as new messages are received.
   3. Display of most recently received message.
   4. User customized display formats.
   5. Limit checking of user selected parameters according to user specified criteria.
   6. Summary displays.
   7. Display of UPD data in its "as received" state without application of any of the user options.

4.2.4.3 Return Channel Time Delay Messages

The SWSI will provide the following RCTD message capabilities:

a. Upon receipt of a RCTD message, the SWSI shall verify that it applies to a SUPIDEN for which there is a logged-on SWSI user. If it does, the SWSI shall notify the user of the receipt of the RCTD message.

b. The SWSI shall store the RCTD message in a file on the Client Workstation such that it is available for later processing by customer applications.

NOTE

In general, RCTD messages will be received only when the return channel time delay option has been specified in a SN return service.

NOTE

A customer application for processing of RCTD data is not part of the SWSI product.

4.2.4.4 Time Transfer Messages

The SWSI will provide the following TTM capabilities:

a. Upon receipt of a TTM, the SWSI shall verify that it applies to a SUPIDEN for which there is a logged-on SWSI user. If it does, the SWSI shall notify the user of the receipt of the TTM.

b. The SWSI shall store the TTM in a file on the Client Workstation such that it is available for later processing by customer applications.

NOTE

> In general, TTMs will be received only when the time transfer option has been specified in a SN tracking service.

NOTE

> A customer application for processing of TTM data is not part of the SWSI product.

4.2.4.5 Acquisition Failure Notification Messages

Upon receipt of an AFN message, the SWSI shall verify that it applies to a SUPIDEN for which there is a logged-on SWSI user. If it does, the SWSI shall notify the user of the receipt of the AFN.

NOTE

> AFN messages are generated by WSC upon failure to acquire a user spacecraft at the scheduled start of a TDRSS return service.

4.2.5 Vector Storage and Transmission

The SWSI will provide the following vector storage and transmission capabilities:

a. Based on the user’s logon information, the SWSI shall provide the user with the capability to select the SIC to be used in vectors from a list of SICs for which the user is authorized.

b. The SWSI shall provide the user with the capability to enter the latitude, longitude, and altitude of a customer spacecraft.

c. The SWSI shall be capable of converting a user-entered set of latitude, longitude, and altitude data for a customer spacecraft into a type 8 (stationary) Improved Interrange Vector (IIRV) for that spacecraft.

d. The SWSI shall provide the user with the capability to directly enter IIRVs.

e. The SWSI shall provide the user with the capability to import files of IIRVs.

f. The SWSI shall provide the user with the capability to select one or more IIRVs for transmission to the NCCDS.

4.3 DAS Interactions

4.3.1 General

4.3.1.1
The SWSI provides SN customers with the capability to interface with the DAS to perform the following functions related to SN services:

a. Service Planning

b. Service Allocation

c. Real-Time Operations

d. Service Performance Monitoring

e. Data Retrieval

f. Customer State Vector Updates

g. Receipt of DAS Alerts

4.3.1.2
In all cases, the SWSI shall ensure that each DAS user is precluded from accessing any other user's messages or data.

4.3.1.3
For each SIC supported by the SWSI, the SWSI shall provide authorized SWSI administrative personnel with the capability to create and maintain all customer data necessary to interact with the DAS. In particular, this will include a set of service specification codes (SSCs) defining the default service configurations for the SIC. For each SIC, the SWSI shall be capable of retaining a minimum of 10 SSCs. The SWSI shall provide the user with the capability to review and reference this data in the process of entering requests.

4.3.2 Service Planning

The SWSI will provide the following DAS service planning capabilities:

a. The SWSI shall provide the user with the capability to request a report on the resource allocations available to the user.

b. Upon receipt of the response from the DAS, the SWSI shall notify the user and make the response available for review.

4.3.3 Service Allocation

The SWSI will provide the following DAS service allocation capabilities:

a. The SWSI shall provide the user with the capability to request the following:

    1. Allocation of a specified resource.
    2. Deletion of a pending or ongoing resource allocation.
    3. Modification of a pending resource allocation.
    4. A list of all currently planned events for the user.
    5. The details of a specified planned event.

b. Upon receipt of the response from the DAS, the SWSI shall notify the user and make the response available for review.

4.3.4 Real-Time Operations

The SWSI will provide the following DAS real-time operations capabilities:

a. The SWSI shall provide the user with the capability to request the following:

    1. Reconfiguration of the values of a specified list of parameters for an ongoing service.
    2. Reacquisition of the return service signal.

b. Upon receipt of the response from the DAS, the SWSI shall notify the user and make the response available for review.

4.3.5 Service Performance Monitoring

The SWSI will provide the following DAS service performance monitoring capabilities:

a. The SWSI shall provide the user with the capability to request that DAS user performance data be enabled or disabled

b. Upon receipt of the response from the DAS, the SWSI shall notify the user and make the response available for review.

c. If user performance data was enabled, the SWSI shall provide this data to the user as it is received from the DAS.

d. The SWSI shall be capable of receiving one DAS user performance data message per minute for each active service with ongoing DAS support.

4.3.6 Data Retrieval

The SWSI will provide the following DAS data retrieval capabilities:

a. The SWSI shall provide the user with the capability to request the following:

    1. A search for archived data within a specified time window.
    2. Playback of specific archived data.
    3. Deletion of a previously playback request.
    4. Modification of a previously playback request.

b. Upon receipt of the response from the DAS, the SWSI shall notify the user and make the response available for review.

4.3.7 Customer State Vector Updates

The SWSI will provide the following DAS state vector update capabilities:

a. The SWSI shall provide the user with the capability to enter and transmit a state vector.

b. Upon receipt of the response from the DAS, the SWSI shall notify the user and make the response available for review.

4.3.8 DAS Alerts

Upon receipt of a DAS alert, the SWSI shall alert the user implied by the SIC specified in the DAS alert message and make the text of the DAS alert message available for review by that user. If the DAS alert message does not apply to a specific user (i.e., SIC = "0000"), the SWSI shall alert all users and make the text of the DAS alert message available for review by all users.

4.4 Database Management

4.4.1 General Features

The SWSI shall provide a database management capability for all SWSI data. The general database management features of the SWSI shall include, but not necessarily be limited to, the following:

a. Data entry, data deletion, data update, and data display.

b. Create, modify, and display data forms and data reports.

c. Make queries, examine data in either form, or file formats.

d. Store both static and dynamic data.

e. Import data from removable media.

f. Export data to removable media.

g. Backup the entire SWSI database.

h. Restore the entire SWSI database.

i. Deposit and query data under the control of SWSI client users.

j. Deposit and query data under the control of SWSI administrative personnel from the SWSI servers.

k. Automatically purge data based on criteria specified by SWSI administrative personnel.

l. Delete data under the direct control of SWSI administrative personnel from the SWSI servers.

4.4.2 SN Service Data

4.4.2.1

The SWSI shall provide all data storage and retrieval capabilities necessary to support the requirements for SN services specified herein. This includes the capability to store and retain requests sent to the NCCDS and to the DAS.

4.4.2.2

For each SIC, the SWSI shall partition data such that some of the data for that SIC can be entered, deleted, or modified only by authorized SWSI administrative personnel while the remainder of the data for that SIC can be entered, deleted, or modified by SWSI client users authorized for that SIC. In general, privileges related to entry, deletion, or modification of relatively static data such as SSCs will be restricted to authorized SWSI administrative personnel while privileges related to entry, deletion, or modification of time-dependent data such as schedule requests will be restricted to SWSI client users.

4.4.2.3

The SWSI shall be capable of automatically purging data related to SN services based on criteria specified by authorized SWSI administrative personnel.

4.4.2.4

The SWSI shall be capable of deleting data related to SN services under the direct control of authorized SWSI client users.

4.4.3 System Data

4.4.3.1

The SWSI shall provide SWSI administrative personnel with the capability to access the contents of server log files.

4.4.3.2

The SWSI shall provide SWSI client users with the capability to access the contents of client log files containing data for which the user is authorized.

4.5 Logging

4.5.1

The SWSI shall be capable of logging and delogging all of the following:

a. Incoming external messages.

b. Outgoing external messages.

c. Alerts sent to SWSI clients.

d. Records pertaining to the establishment and termination of communications connections.

e. Records pertaining to SWSI system failures.

f. Records pertaining to SWSI database failures.

g. Records pertaining to successful SWSI logon attempts.

h. Records pertaining to rejected SWSI logon attempts.

4.5.2
The SWSI shall provide SWSI administrative personnel with the capability to selectively control the logging and delogging of all of the above.

4.5.3
The SWSI shall provide SWSI client users with the capability to selectively control delogging of all of the above data for which the user is authorized.

4.6 System Performance

4.6.1
The SWSI shall have the capacity to store data for a minimum of 100 customer spacecraft. The SWSI shall allow for one set of operational data and for at least one set of test data for each spacecraft.

4.6.2
For any combination of Internet, Open IONet and Closed IONet SWSI clients, the SWSI servers shall be capable of supporting simultaneous connections with a minimum of fifty SWSI clients.

4.6.3
In general, actual SWSI response times depend on factors that are beyond the control of the SWSI product. The following response time requirements apply to the performance of the SWSI product, itself, and exclude delays due to factors such as IONet traffic volume and the performance of the SWSI client infrastructure. This limited set of response time requirements is intended only to characterize the overall performance of the SWSI, and not to provide a comprehensive set of response time requirements. Other specific interactions should have comparable response times.

a. For interactions initiated from the SWSI client and requiring a response from the NCCDS or DAS, the SWSI response time from the perspective of the SWSI client shall not be more than 10 seconds greater than the NCCDS or DAS response time from the perspective of the SWSI backend server.

b. For interactions initiated from the SWSI client and requiring simple retrieval of data from the SWSI database, the SWSI response time from the perspective of the SWSI client shall not be greater than 10 seconds.

NOTE

"Simple retrieval" applies to an action such as retrieving a single scheduled SN event. It does not apply to a complex action such as retrieval of an entire schedule.

Section 5. Operations and Maintenance

5.1 General

5.1.1
The SWSI servers shall be capable of continuous unattended operation.

5.1.2
The SWSI servers shall be designed and configured such that routine system maintenance operations and routine system administrative functions can be executed without rendering the capabilities of the servers operationally unavailable to the SWSI clients.

5.2 Reliability, Maintainability, and Availability

5.2.1 Reliability

5.2.1.1
The measure of reliability for the SWSI servers is the Mean Time Between Failures (MTBF). The MTBF is defined as the 10-year life cycle of a fully operational SWSI divided by the predicted number of failures. The MTBF is determined in accordance with MIL-HDBK-217, Reliability Prediction of Electronic Equipment.

5.2.1.2
The Parts Count Reliability prediction method of MIL-HDBK-217 shall be used in the initial stages of system design.

5.2.1.3
The reliability prediction method shall shift to the Parts Stress Analysis Prediction method, or other reliability modeling technique approved by NASA, at the time when a firm, detailed parts list is available.

5.2.1.4
The MTBFs of the SWSI servers shall be determined in accordance with MIL-HDBK-217, Reliability Prediction of Electronic Equipment.

5.2.2 Maintainability

The maintainability requirement for the SWSI servers is stated in terms of Mean Time To Repair (MTTR). The MTTR is the quotient obtained by dividing the sum of the times to repair failures by the number of failures. Excluded from time to repair are the time to obtain parts, components, tools, or supplies not provisioned at the SWSI facility, the time for essential personnel not scheduled to be at the SWSI facility to be notified of the failure and to travel to the SWSI facility, and the time to develop and configure software corrections. Based on the preceding definitions, the SWSI servers shall have an MTTR no greater than 60 minutes.

5.2.3 Availability

5.2.3.1 Inherent Availability

5.2.3.1.1
Inherent Availability (Ai) is the probability that a system or equipment, when used under stated conditions in an ideal support environment (i.e., using available tools, spares, and personnel) will operate within specifications at all times. It excludes preventive maintenance actions, logistics supply time, and administrative downtime and is expressed as: Ai = MTBF/(MTBF + MTTR).

5.2.3.1.2
The inherent availability of any individual SWSI server for any period of 10,000 hours shall be 0.9998.

5.2.3.2 Operational Availability

5.2.3.2.1
The Operational Availability (Ao) of the SWSI servers is defined in terms of the availability of the SWSI backend servers to the SWSI Open IONet clients excluding any times during which the SWSI backend servers are unavailable due to failure of the Open IONet, the Closed IONet, or the IONet Secure Gateway.

5.2.3.2.2
SWSI operational availability for any period of 10,000 hours interval shall be 0.9999. Redundant paths may be used in achieving this Ao.

5.3 System Maintenance

This section contains the detailed maintenance requirements for the SWSI. The objective of the maintenance functions is to support achievement of the required inherent availability. General requirements, which directly affect the performance of maintenance functions, include ease of access to equipment for tests and maintenance, the use of built-in test and diagnostic features, and the capability to perform maintenance without interfering with on-going operations.

The SWSI shall have the resources, personnel, and logistics support required to maintain, modify, and repair hardware and maintain modify and enhance software. Hardware maintenance is performed under a formally established system maintenance program that includes both Preventive Maintenance and Corrective Maintenance procedures.

5.3.1 General Requirements

a. The contractor shall develop procedures using 500-TIP-2111, Content Specification for Operation and Maintenance Manuals, as a guideline.

b. Any state-of-the-art techniques that are developed for the SWSI shall be included in the procedures.

5.3.2 Hardware Maintenance

Hardware maintenance will be conducted at two levels. First level maintenance is conducted to support the inherent availability requirements by replacement of Line Replaceable Units (LRUs) and line replaceable items within LRUs. Second level maintenance consists of the repair, adjustment, and testing of LRUs removed from service during first level maintenance actions. Attention will be given to GSFC specifications so as to provide for chassis slides, cable service loops, and cable retractors to aid maintenance. The following are requirements for hardware maintenance:

5.3.2.1 Identification of LRU

LRUs shall include rack-mounted equipment drawers and panels and other assemblies that can be removed by unplugging power and signal connectors without physically disturbing other LRUs. Other line replaceable items include printed circuit cards and other plug-in components within an LRU.

5.3.2.2 First Level Maintenance

a. First level maintenance will include scheduled preventive maintenance.

b. First level maintenance will include fault isolating to the level of an LRU.

c. Fault isolation to the level of a line replaceable item within an LRU (if any) shall be performed if the time required is consistent with the operational maintainability requirement.

d. First level maintenance shall include replacement of a failed LRU or line replaceable element within an LRU.

e. First level maintenance shall include testing to ensure that the system/subsystem has been restored to operational condition.

f. First level maintenance will include alignment and tuning.

5.3.2.3 Second Level Maintenance

Second level maintenance is conducted to restore malfunctioning equipment to serviceable condition when the failure requires unit/element disassembly. Second level maintenance is also required when the fault isolation capabilities of first level maintenance are incapable of localizing a failure to a line replaceable item within an LRU. Second level maintenance is performed in or under the management control of the Hardware Maintenance Depot. The requirements are as follows:

a. Second level maintenance actions will include localization of a failure to the piece-part or equipment component level, as appropriate.

b. Second level maintenance actions will include disassembly and removal of the failed piece-part or equipment component.

c. Second level maintenance actions will include replacement of failed elements and reassembly.

d. Second level maintenance actions will include bench testing to ensure performance to the specified level.

5.3.3 Software Maintenance

Software maintenance, including debugging, modification, and enhancement of system software packages, will be performed in the Software Maintenance. The requirements are:

5.3.3.1

SWSI system shall provide capability for personnel to be cognizant of anomalous software behavior.

5.3.3.2

SWSI system shall provide capability for personnel to initiate software trouble reports.

5.3.3.3

SWSI system shall provide capability for personnel to install vendor-supplied software fixes and upgrades.

5.3.4 Spares

SWSI shall be configured redundantly (e.g., a prime and a backup) for both Open and Closed IONet. Therefore, there is no requirement for maintaining an on-site supply of spare components.

Section 6. Documentation

6.1

SWSI operations personnel shall be provided with all documentation needed to perform the functions indicated above.

6.2

All documentation shall be developed in accordance with the Data Requirements List (DRL) and Data Item Descriptions (DIDs). The DRL lists each document to be provided and the DIDs describe the purpose, content, and format of each document.

6.3

Document requirements list (TBS).

Section 7. Training

7.1 General

This subsection specifies the SWSI project objectives and approach for training of SWSI operations and maintenance personnel. The training policies, plans, and procedures shall provide for orderly transition into sustained operations and maintenance.

7.1.1 General Requirements

7.1.1.1
The training program shall include a definition of the qualifications required by operations and maintenance personnel to meet position description skill requirements.

7.1.1.2
A training plan to define the phasing, methods and techniques for achieving the requisite skill levels, using curricula and course materials for skill/qualification areas within each position description shall be included.

7.1.1.3
Training devices and equipment shall be included.

7.1.1.4
Administrative support to implement the training program shall be included.

7.1.2 Skill Area Requirements

7.1.2.1 Operator Training

a. Operator training shall cover the SWSI network overview.

b. Operator training shall cover the SWSI concept of operation.

c. Operator training shall cover detailed SWSI operational procedure.

7.1.2.2 Maintenance Training

a. Maintenance training for both hardware and software shall cover the SWSI maintenance concept.

b. Maintenance training for both hardware and software shall cover diagnostics and troubleshooting.

c. Maintenance training for both hardware and software shall cover detailed repair procedures and techniques including the use of available tools and repair equipment.

d. Maintenance training for both hardware and software shall cover SWSI software maintenance concepts.

e. Software maintenance training shall include debugging techniques.

f. Training shall cover maintenance of both operational and support software.

7.1.3 Training Devices and Equipment

7.1.3.1

SWSI training devices and equipment for maintenance training shall be specified in the Training Plan.

7.1.4 Training Support

7.1.4.1

Administrative support for training shall provide for the testing and certification of students.

Abbreviations and Acronyms

Ai	Inherent Availability
ANCC	Auxiliary Network Control Center
Ao	operational availability
ASAR	Alternate Schedule Add Request
BB	bit block
CNE	Center Network Environment
DAS	Demand Access System
DBMS	Database Management System
DID	Data Item Descriptions
DRL	Data Requirements List
DSMC	Data Services Management Center
EIRP	Effective Isotropic Radiated Power
GCM	Ground Control Message
GCMR	Ground Control Message Request
GSFC	Goddard Space Flight Center
GUI	Graphical User Interface
HP	Hewlett-Packard
ICD	Interface Control Document
IIRV	Improved Inter-Range Vectors
IONet	Internet Protocol Operational Network
IP	Internet Protocol
IT	Information Technology
LDBP	Long Duration Balloon Project
LRU	line replaceable unit
MAR	Multiple Access Return
MOC	Mission Operations Center
MSOCC	Multisatellite Operations Control Center
MTBF	mean time between failures

MTTR	mean time to repair
N/A	Not Applicable
NASA	National Aeronautics and Space Administration
NCC	Network Control Center
NCCDS	Network Control Center Data System
NISN	NASA Integrated Services Network
NPG	NASA Procedures and Guidelines
O&M	Operations & Maintenance
ODIN	Outsourcing Desktop Initiative for NASA
PCD	Project Commitment Document
RCTD	Return Channel Time Delay
RMA	Reliability, Maintainability, and Availability
RR	Replace Request
SAR	Schedule Add Request
SDR	Schedule Delete Request
SIC	Spacecraft Identification Code
SN	Space Network
SRM	Schedule Result Message
STDN	Spaceflight Tracking and Data Network
SWSI	Space Network Web Services Interface
SUPIDEN	Support Identifier
TBS	to be supplied
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDRS	Tracking and Data Relay Satellite
TSW	TDRS Scheduling Window

TTM	Time Transfer Message
TUT	TDRSS Unscheduled Time
UPD	User Performance Data
UPS	User Planning System
USM	User Schedule Message
WAN	Wide Area Network
WLR	Wait List Request

CHANGE HISTORY LOG

Revision	Effective Date	Description of changes
Baseline CCR # 453/035	February 2001	Initial Release

453-SRD-SWSI

Space Network Web Services Interface System Requirements

Original